United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

UNITED STATES OF AMERICA, Plaintiff, v. JONATHAN JOSEPH NELSON, *et al.*, Defendants.	Case No. 17-cr-00533-EMC (LB) **ORDER REGARDING ELECTRONIC DISCOVERY**

This order memorializes the court's and the parties' discussions regarding electronic discovery at the March 14, 2019 discovery hearing and the court's decisions relating to electronic discovery.

The government has turned over the contents of 115 electronic devices that it seized. It produced the contents of 14 devices as Cellebrite reports and 101 devices as EnCase extractions.[1] On March 8, 2019, the defense filed a status report stating that it was satisfied with the production of the contents of the 14 devices produced as Cellebrite reports but raising issues regarding the contents of the 101 devices produced as EnCase extractions.[2]

[1] Def. ESI Status Report – ECF No. 594 at 2. Citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

[2] *Id.* at 2–4.

At the March 14 hearing, the government said that the EnCase extractions it produced are full forensic images of their respective devices. The government also said that agents are in the process of identifying items in the extractions that are responsive to the search warrants and that, as those reports are created, the government will produce them to the defense.[3]

At the March 14 hearing, the defense said that it is able to mount the EnCase extractions using free available software called FTK (Forensic Tool Kit) Imager and see a list of the files in the EnCase extractions (i.e., the files extracted from the devices).[4] The defense also said that it can open the files in EnCase extractions, if it has the proper programs that can read those files (e.g., it can open and view any Microsoft Word files or JPEG photo files included in an EnCase extraction because it has Microsoft Word software and photo-viewing software).

The defense mentioned that it cannot open files in EnCase extractions when it does not have the proper program (e.g., it cannot open an .xyz file without having a program that can read .xyz files). That is a separate issue from the accessibility of the EnCase extractions themselves. The defense does not appear to claim that there is any EnCase extraction that it cannot mount. As for any hypothetical .xyz files, the court is not sure that this is actually a live issue now, but if it is, the parties must meet and confer on solutions.[5]

The defense also argues that there are hundreds of thousands of files in the EnCase extractions.[6] That is a function of the fact that (1) there were that many files on the original devices and (2) the government is producing the full contents of the devices to the defense. (For

---

[3] The defense stated that the government has produced two forensic-report files to the defense to date. *Id.* at 3. At the March 14 hearing, the government said that it will make rolling productions of further reports as they are created and estimates that it may take eight months to finish its review.

[4] An EnCase extraction comes as a file with the extension .e01. *Id.* at 2–3. FTK Imager can be used to "mount" the EnCase extraction as a virtual drive. A viewer can then access the files in the extraction.

[5] The court notes that it would be unreasonable to require the government to index in advance the full contents of the EnCase extracts and to identify in advance how to open any hypothetical .xyz file, particularly if the government is not able to open .xyz files either. *Cf. United States v. Skilling*, 554 F.3d 529, 577 (5th Cir. 2009) (rejecting argument that "the government should have scoured the open file in search of exculpatory information to provide to [defendant]" where "the government was in no better position to locate any potentially exculpatory evidence than was [defendant]"), *aff'd in part and vacated in part on other grounds*, 561 U.S. 358 (2010). If there are issues with specific files, the parties must meet and confer.

[6] *Id.* at 4.

example, if someone took a thousand photos with his cell phone, the EnCase extraction of that cell phone would have a thousand photo files.) That is the nature of forensic production. The government ultimately will produce reports identifying the items in the extractions that the agents identify as responsive to search warrants. That will be a more limited universe of documents. And, as discussed at the hearing, if the defense is not satisfied with the government's identification of documents or does not want to wait, it can conduct its own reviews within the full EnCase extractions. In sum, the information here is available to the defense through the exercise of reasonable diligence. *Cf. United States v. Skilling*, 554 F.3d 529, 576–77 (5th Cir. 2009), *aff'd in part and vacated in part on other grounds*, 561 U.S. 358 (2010); *United States v. AU Optronics Corp.*, No. C 09-110 SI, 2011 WL 6778520, at *1–2 (N.D. Cal. Dec. 23, 2011).[7]

If there are further disputes regarding the government's electronic-discovery productions, the parties must meet and confer.

IT IS SO ORDERED.

Dated: March 15, 2019

LAUREL BEELER
United States Magistrate Judge

[7] It might be more efficient if the government, as it conducts its review of the extracts, were to produce indices, or a set of "hot documents" that it thought were particularly important to its case or the defendants' defenses, *cf. Skilling*, 554 F.3d at 577, but on this record, the court cannot order more. *Cf. AU Optronics*, 2011 WL 6778520, at *1–2.